Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MANUEL CAMPOS SÁNCHEZ-BORDONA
présentées le 12 mai 2016 [1]

**Affaire C-582/14**

**Patrick Breyer**
**contre**
**Bundesrepublik Deutschland**

[demande de décision préjudicielle formée par le Bundesgerichtshof (Cour fédérale de justice, Allemagne)]

«Traitement de données à caractère personnel — Directive 95/46/CE — Article 2, sous a), et article 7, sous f) — Notion de "données à caractère personnel" — Adresses IP (protocole Internet) — Conservation par un fournisseur de médias électroniques — Réglementation nationale ne permettant pas la prise en compte de l'intérêt légitime poursuivi par le responsable du traitement»

1. Une adresse IP (protocole Internet) est une suite de chiffres binaires qui, attribuée à un dispositif (ordinateur, tablette, téléphone intelligent), l'identifie et lui permet d'accéder au réseau de communications électroniques. Pour se connecter à Internet, le dispositif doit utiliser la suite de chiffres donnée par les fournisseurs du service d'accès au réseau. L'adresse IP est communiquée au serveur sur lequel le site Internet consulté est hébergé.

2. En particulier, les fournisseurs d'accès au réseau (généralement les entreprises de téléphonie) attribuent à leurs clients les adresses dites « adresses IP dynamiques » de manière provisoire, pour chaque connexion à Internet, et les modifient lors des connexions ultérieures. Ces entreprises tiennent un registre dans lequel figure l'adresse IP qu'elles ont attribuée, à chaque fois, à un dispositif déterminé [2].

3. Les propriétaires des sites Internet consultés au moyen des adresses IP dynamiques tiennent généralement aussi des registres indiquant les sites consultés, le moment où ils l'ont été et l'adresse IP à partir de laquelle la consultation a eu lieu. Ces registres peuvent, techniquement, être conservés sans limite de temps après la fin de la connexion à Internet de chaque utilisateur.

4. Une adresse IP dynamique ne suffit pas, à elle seule, pour que le fournisseur de services identifie l'utilisateur de son site Internet. Toutefois, il pourrait le faire s'il combinait l'adresse IP dynamique à d'autres informations détenues par le fournisseur d'accès au réseau.

1 — Langue originale : l'espagnol.

2 — L'article 5 de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), imposait, entre autres obligations, de conserver, aux fins de la recherche, de la détection et de la poursuite d'infractions graves, « la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet […], ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit ».

5. Le point litigieux en l'espèce est de savoir si les adresses IP dynamiques sont une donnée à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46/CE [3]. La réponse exige de déterminer, préalablement, la pertinence, à cette fin, du fait que les informations supplémentaires nécessaires pour identifier l'utilisateur soient en possession non pas du propriétaire du site Internet, mais d'un tiers (en l'occurrence, le fournisseur du service d'accès au réseau).

6. Il s'agit d'une question inédite pour la Cour. Au point 51 de l'arrêt Scarlet Extended [4], celle-ci a certes déclaré que les adresses IP sont « des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs », mais dans un contexte dans lequel la collecte et l'identification des adresses IP étaient faites par le fournisseur d'accès au réseau [5], et non par un fournisseur de contenus, comme c'est le cas en l'espèce.

7. Si les adresses IP dynamiques étaient, pour le fournisseur de services Internet, des données à caractère personnel, il conviendrait d'examiner si leur traitement relève du champ d'application de la directive 95/46.

8. Même si elles étaient des données personnelles, il serait possible qu'elles ne jouissent pas de la protection découlant de la directive 95/46, si, par exemple, la finalité de leur traitement était l'exercice d'actions pénales contre d'éventuels auteurs d'attaques contre le site Internet. Dans cette hypothèse, la directive 95/46 n'est pas applicable, conformément à l'article 3, paragraphe 2, premier tiret.

9. Il convient en outre de déterminer si le fournisseur de services qui enregistre les adresses IP dynamiques lorsqu'un utilisateur accède à ses sites Internet (en l'espèce la République fédérale d'Allemagne) agit en tant que pouvoir public ou en tant que particulier.

10. Si la directive 95/46 était applicable, il y aurait enfin lieu de préciser jusqu'à quel point l'article 7, sous f), de ce texte est compatible avec une réglementation nationale qui restreint la portée de l'une des conditions fixées dans cette disposition pour justifier le traitement de données à caractère personnel.

## I – Le cadre juridique

### A – *Le droit de l'Union*

11. Le considérant 26 de la directive 95/46 est libellé comme suit :

« (26) considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable ; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable ; que les codes de conduite au sens de l'article 27 peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée ».

3 — Directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

4 — Arrêt du 24 novembre 2011 (C-70/10, EU:C:2011:771, point 51).

5 — C'était également le cas dans l'arrêt du 19 avril 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219, points 51 et 52).

12. Aux termes de l'article 1er de la directive 95/46 :

« 1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1. »

13. Aux termes de l'article 2 de la directive 95/46 :

« Aux fins de la présente directive, on entend par :

a) "données à caractère personnel" : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

b) "traitement de données à caractère personnel" (traitement) : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

[…]

d) "responsable du traitement" : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ;

[…]

f) "tiers" : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ;

[…] ».

14. Sous le titre « Champ d'application », l'article 3 de la directive 95/46 prévoit ce qui suit :

« 1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel :

— mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

[…] »

15. Le chapitre II de la directive 95/46, portant sur les conditions générales de licéité des traitements de données à caractère personnel, commence par l'article 5, aux termes duquel « [l]es États membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites ».

16. Aux termes de l'article 6 de la directive 95/46 :

1. Les États membres prévoient que les données à caractère personnel doivent être :

a) traitées loyalement et licitement ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

d) exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1. »

17. Conformément à l'article 7 de la directive 95/46 :

« Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

a) la personne concernée a indubitablement donné son consentement

ou

b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

ou

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

ou

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

ou

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, paragraphe 1. »

18. L'article 13 de la directive 95/46 dispose ce qui suit :

« 1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6, paragraphe 1, à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder :

a) la sûreté de l'État ;

b) la défense ;

c) la sécurité publique ;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées ;

e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) ;

g) la protection de la personne concernée ou des droits et libertés d'autrui.

[…] »

B – *Le droit allemand*

19. L'article 12 de la Telemediengesetz (loi sur les médias électroniques) [6] prévoit ce qui suit :

« 1. Le fournisseur de services ne peut collecter et utiliser des données à caractère personnel aux fins de la mise à disposition de médias électroniques que si la présente loi ou un autre instrument juridique qui vise expressément les médias électroniques l'autorise ou si l'utilisateur y a consenti.

2. Le fournisseur de services ne peut utiliser les données à caractère personnel collectées aux fins de la mise à disposition de médias électroniques à d'autres fins que si la présente loi ou un autre instrument juridique qui vise expressément les médias électroniques l'autorise ou si l'utilisateur y a consenti.

3. Sauf dispositions contraires, la législation en vigueur régissant la protection des données à caractère personnel doit être appliquée même si les données ne font pas l'objet d'un traitement automatisé. »

20. Aux termes de l'article 15 de la TMG :

« 1. Le fournisseur de services ne peut collecter et utiliser des données à caractère personnel d'un utilisateur que dans la mesure où cela est nécessaire pour permettre et facturer l'utilisation des médias électroniques (données d'utilisation). Les données d'utilisation sont en particulier :

1) les critères permettant l'identification de l'utilisateur,

2) les indications sur le début et la fin de chaque utilisation, ainsi que son étendue,

3) les indications sur les médias électroniques utilisés par l'utilisateur.

2. Le fournisseur de services peut regrouper les données d'utilisation d'un même utilisateur, relatives à l'utilisation de différents médias électroniques, dans la mesure où cela est nécessaire à des fins de facturation à l'utilisateur.

[…]

4. Le fournisseur de services peut utiliser les données d'utilisation après la fin de la session dans la mesure où cela est nécessaire pour la facturation de la prestation à l'utilisateur (données de facturation). Afin de respecter des délais de conservation légaux, statutaires ou contractuels, le fournisseur de services peut verrouiller les données. […] »

21. Conformément à l'article 3, paragraphe 1, de la Bundesdatenschutzgesetz (loi fédérale sur la protection des données) [7], « [l]es données à caractère personnel sont des données particulières sur des situations personnelles ou matérielles d'une personne physique identifiée ou identifiable (personne concernée) ».

## II – Les faits

22. M. Patrick Breyer a engagé une action en cessation de l'enregistrement d'adresses IP contre la République fédérale d'Allemagne.

6 — Loi du 26 février 2007 (BGBl. 2007 I, p. 179, ci-après la « TMG »).

7 — Loi du 20 décembre 1990 (BGBl. 1990 I, p. 2954, ci-après la « BDSG »).

23. De nombreuses institutions publiques allemandes ont des portails Internet accessibles au public sur lesquels elles fournissent des informations actualisées. Afin de se prémunir contre les attaques et de rendre possibles les poursuites pénales contre les pirates, la plupart de ces portails enregistrent toutes les consultations dans des fichiers ou des registres de protocole. Y sont conservés, y compris après la fin de la session, le nom du site ou du fichier consulté, les termes entrés dans les champs de recherche, la date et l'heure de la consultation, le volume des données transférées, la constatation du succès de la consultation et l'adresse IP de l'ordinateur à partir duquel la consultation a été faite.

24. M. Breyer, qui a consulté plusieurs des sites mentionnés, a demandé, dans son recours, que la République fédérale d'Allemagne soit condamnée à cesser d'enregistrer ou de faire enregistrer par des tiers l'adresse IP du système hôte à partir duquel la consultation a eu lieu, dans la mesure où cela n'est pas nécessaire aux fins du rétablissement de la disponibilité du média électronique en cas de dérangement.

25. Le recours de M. Breyer a été rejeté en première instance. Il a toutefois été partiellement fait droit à son recours en appel, la République fédérale d'Allemagne ayant été condamnée à cesser l'enregistrement après la fin de chaque session. L'ordre de cessation a été subordonné au fait que le requérant ait fourni ses données à caractère personnel pendant une session, y compris sous la forme d'une adresse électronique, et au caractère non nécessaire de l'enregistrement aux fins du rétablissement de la disponibilité du média électronique.

## III – Les questions préjudicielles

26. Les deux parties ayant formé un pourvoi en « Revision », la sixième chambre du Bundesgerichtshof (Cour fédérale de justice, Allemagne) a posé les questions préjudicielles suivantes le 17 décembre 2014 :

« 1) L'article 2, sous a), de la directive 95/46/CE […] doit-il être interprété en ce sens qu'une adresse de protocole Internet (adresse IP) qui est enregistrée par un fournisseur de services à l'occasion d'un accès à son site Internet constitue pour celui-ci une donnée à caractère personnel même si c'est un tiers (en l'occurrence, le fournisseur d'accès) qui dispose des informations supplémentaires nécessaires pour identifier la personne concernée ?

2) L'article 7, sous f), de la directive 95/46 s'oppose-t-il à une disposition de droit national en vertu de laquelle le fournisseur de services ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur sans le consentement de celui-ci que dans la mesure où cela est nécessaire pour permettre et facturer l'utilisation concrète du média électronique par l'utilisateur en question et en vertu de laquelle la finalité consistant à garantir la capacité générale de fonctionnement du média électronique ne peut pas justifier l'utilisation des données après la fin de la session en cours ? »

27. Comme l'explique la juridiction de renvoi, le requérant pourrait exiger, conformément au droit allemand, que la défenderesse cesse d'enregistrer les adresses IP si leur conservation constituait une atteinte illégale, au regard du droit de la protection des données, à ses droits généraux de la personnalité, notamment à son droit à « l'autodétermination informationnelle » [dispositions combinées de l'article 1004, paragraphe 1, et de l'article 823, paragraphe 1, du Bürgerliches Gesetzbuch (code civil allemand), ainsi que des articles 1er et 2 de la Grundgesetz (loi fondamentale)].

28. Il en serait ainsi a) si l'adresse IP (en tout cas accompagnée de la date de l'accès à un site Internet) pouvait être qualifiée de « donnée à caractère personnel » au sens des dispositions combinées de l'article 2, sous a), et du considérant 26, deuxième membre de phrase, de la directive 95/46 ou des dispositions combinées de l'article 12, paragraphes 1 et 3, de la TMG et de l'article 3, paragraphe 1, de la BDSG, et b) si cela n'était pas autorisé au sens de l'article 7, sous f), de la directive 95/46 ou de l'article 12, paragraphes 1 et 3, et de l'article 15, paragraphes 1 et 4, de la TMG.

29. Selon le Bundesgerichtshof (Cour fédérale de justice), il est indispensable, aux fins d'interpréter le droit national (article 12, paragraphe 1, de la TMG), de savoir ce qu'il y a lieu d'entendre par le caractère personnel des données visées à l'article 2, sous a), de la directive 95/46.

30. La juridiction de renvoi indique en outre que, puisque, aux termes de l'article 15, paragraphe 1, de la TMG, le fournisseur de services ne peut collecter et utiliser des données à caractère personnel d'un utilisateur que dans la mesure où cela est nécessaire pour permettre et facturer l'utilisation des médias électroniques (données d'utilisation) [8], l'interprétation de cette disposition nationale dépend de celle de l'article 7, sous f), de la directive 95/46.

## IV – La procédure devant la Cour, les allégations des parties

31. Des observations écrites ont été déposées par les gouvernements allemand, autrichien et portugais ainsi que par la Commission européenne. Seuls cette institution et M. Breyer ont comparu lors de l'audience qui s'est tenue le 25 février 2016, à laquelle le gouvernement allemand n'a pas souhaité participer.

### A – *Les allégations des parties relativement à la première question*

32. Selon M. Breyer, constituent également des données à caractère personnel celles dont la combinaison n'est possible que d'un point de vue théorique, c'est-à-dire en se fondant sur un risque potentiel abstrait, le point de savoir si cette combinaison est effectivement mise en œuvre important peu. Selon lui, le fait qu'un organisme puisse être relativement incapable d'identifier une personne à l'aide de l'adresse IP ne signifie pas une absence de risque pour cette personne. En outre, M. Breyer attache une importance au fait que la République fédérale d'Allemagne conserve ses données IP afin, le cas échéant, d'identifier d'éventuelles attaques ou d'engager des actions pénales, comme le permet l'article 113 de la Telekommunikationsgesetz (loi sur les télécommunications) et comme cela a eu lieu à plusieurs occasions.

33. Pour le gouvernement allemand, il convient de répondre à la première question par la négative. Selon lui, les adresses IP dynamiques ne révèlent pas une « personne identifiée » au sens de l'article 2, sous a), de la directive 95/46. Pour établir si elles donnent des informations sur une personne « identifiable » au sens de cette disposition, l'examen de l'« *identificabilité* » doit être effectué sur la base d'un critère « relatif ». C'est ce qui ressort, selon lui, du considérant 26 de la directive 95/46, aux termes duquel seuls les moyens susceptibles d'être « raisonnablement » mis en œuvre soit par le responsable du traitement, soit par un tiers, pour identifier une personne doivent être pris en compte. Cette précision montrerait que le législateur de l'Union n'a pas souhaité faire entrer dans le champ d'application de la directive 95/46 les situations dans lesquelles une identification est objectivement possible par n'importe quel tiers.

8 — Selon le Bundesgerichtshof (Cour fédérale de justice), les données d'utilisation sont les critères permettant l'identification de l'utilisateur, les indications sur le début et la fin de chaque utilisation, ainsi que son étendue, et les indications sur les médias électroniques utilisés par l'utilisateur.

34. Le gouvernement allemand considère également que la notion de « données à caractère personnel », au sens de l'article 2, sous a), de la directive 95/46, doit être interprétée à la lumière de la finalité de cette directive consistant à garantir le respect des droits fondamentaux. Le besoin de protection des personnes physiques pourrait se présenter de manière différente en fonction de la personne qui détient les données et du point de savoir si cette dernière dispose ou non des moyens de s'en servir aux fins d'identifier les personnes physiques.

35. Le gouvernement allemand affirme que M. Breyer n'est pas identifiable sur la base des adresses IP combinées aux autres données conservées par les fournisseurs de contenus. Il faudrait pour cela manipuler l'information détenue par les fournisseurs d'accès à Internet, qui, en l'absence de base légale, ne peuvent la fournir aux fournisseurs de contenus.

36. Pour le gouvernement autrichien, il convient au contraire de répondre à la première question par l'affirmative. Conformément au considérant 26 de la directive 95/46, pour qu'une personne soit considérée comme identifiable, il n'est pas nécessaire que tous les moyens d'identification de cette personne se trouvent entre les mains d'une seule entité. Ainsi, une adresse IP pourrait constituer une donnée à caractère personnel si un tiers (par exemple, le fournisseur d'accès à Internet) dispose des moyens nécessaires à l'identification du titulaire de cette adresse sans déployer d'efforts démesurés.

37. Le gouvernement portugais tend également à répondre par l'affirmative à la première question. Il estime que l'adresse IP constitue, en combinaison avec la date de session de consultation, une donnée à caractère personnel, dans la mesure où elle peut conduire à l'identification de l'utilisateur par une entité autre que celle qui a conservé l'adresse IP.

38. La Commission propose également de répondre par l'affirmative, en s'appuyant sur la solution adoptée par la Cour dans l'affaire Scarlet Extended[9]. Pour la Commission, puisque l'enregistrement des adresses IP sert précisément à l'identification des utilisateurs en cas d'attaques cybernétiques, l'utilisation des données supplémentaires enregistrées par les fournisseurs d'accès à Internet constituerait un moyen qui peut être « raisonnablement » mis en œuvre, au sens du considérant 26 de la directive 95/46. En définitive, selon la Commission, l'objectif de la directive 95/46 ainsi que les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») plaident en faveur d'une interprétation large de l'article 2, sous a), de la directive 95/46.

### B – *Les allégations des parties relativement à la seconde question*

39. M. Breyer considère que l'article 7, sous f), de la directive 95/46 constitue une clause générale dont la mise en œuvre requiert matérialisation. Conformément à la jurisprudence de la Cour, il conviendrait donc d'apprécier les circonstances au cas par cas et de déterminer s'il existe des groupes ayant un intérêt légitime, au sens de cette disposition, auquel cas il serait non seulement permis, mais indispensable, de prévoir des règles spécifiques à l'égard de ces groupes, aux fins de l'application de cet article. M. Breyer considère que, dans une telle hypothèse, la réglementation nationale serait conforme à l'article 7, sous f), de la directive 95/46, puisqu'il n'existe pas d'intérêt du portail public à conserver des données à caractère personnel ou parce que l'intérêt à protéger l'anonymat prévaut. Selon lui, une conservation systématique et personnelle des données n'est néanmoins ni conforme à une société démocratique ni nécessaire et proportionnée pour garantir le fonctionnement des médias électroniques, tout à fait possible sans enregistrement de ces données à caractère personnel, comme le démontreraient les sites Internet de certains ministères fédéraux.

40. Le gouvernement allemand estime qu'il n'y a pas lieu de répondre à la seconde question, qui n'a été posée que dans l'hypothèse d'une réponse affirmative à la première question, ce qui, selon lui, n'est pas le cas, pour les raisons précitées.

9 — Arrêt du 24 novembre 2011 (C-70/10, EU:C:2011:771, point 51).

41. Le gouvernement autrichien propose de répondre en ce sens que la directive 95/46 ne s'oppose pas de manière générale à la conservation de données telles que celles en cause au principal si cela est nécessaire pour garantir le bon fonctionnement des médias électroniques. Selon ce gouvernement, une conservation limitée de l'adresse IP au-delà de la durée de consultation d'un site Internet peut être licite, au regard de l'obligation pour le responsable du traitement des données à caractère personnel d'appliquer les mesures de protection de ces données imposées à l'article 17, paragraphe 1, de la directive 95/46. La lutte contre les attaques cybernétiques pourrait justifier l'analyse des données relatives à des attaques antérieures et le refus de l'accès au site Internet à certaines adresses IP. La proportionnalité de la conservation de données telles que celles en cause au principal au regard de l'objectif visant à assurer le bon fonctionnement des médias électroniques devrait être appréciée au cas par cas, en tenant compte des principes énoncés à l'article 6, paragraphe 1, de la directive 95/46.

42. Le gouvernement portugais considère que l'article 7, sous f), de la directive 95/46 ne s'oppose pas aux règles du droit national en cause au principal, car le législateur allemand aurait déjà effectué la pondération, prévue à cette disposition, entre, d'une part, les intérêts légitimes du responsable du traitement des données à caractère personnel et, d'autre part, les droits et les libertés des titulaires de ces données.

43. Pour la Commission, la réglementation nationale qui transpose l'article 7, sous f), de la directive 95/46 doit définir les objectifs du traitement de données à caractère personnel de manière à ce qu'ils soient prévisibles pour le particulier concerné. Selon elle, la réglementation allemande ne respecte pas cette exigence en prévoyant, à l'article 15, paragraphe 1, de la TMG, que la conservation des adresses IP est autorisée « dans la mesure où cela est nécessaire pour permettre […] l'utilisation des médias électroniques ».

44. La Commission propose donc de répondre à la seconde question en ce sens que l'article 7, sous f), de la directive 95/46 s'oppose à l'interprétation d'une disposition nationale selon laquelle une autorité publique agissant en tant que fournisseur de services peut collecter et utiliser les données à caractère personnel d'un utilisateur sans son consentement, même si l'objectif est d'assurer le bon fonctionnement général du média électronique, si la disposition nationale n'établit pas cet objectif de manière suffisamment claire et précise.

## V – Appréciation

### A – *Sur la première question*

#### 1. Délimitation de la question posée

45. Dans les termes dans lesquels le Bundesgerichtshof (Cour fédérale de justice) l'a formulée, la première de ses questions préjudicielles vise à savoir si une adresse IP permettant d'accéder à un site Internet constitue, pour l'entité publique propriétaire de ce site, une donnée à caractère personnel [au sens de l'article 2, sous a), de la directive 95/46] dans le cas où le fournisseur d'accès au réseau possède des informations supplémentaires permettant l'identification de l'intéressé.

46. Ainsi rédigée, la question est suffisamment précise pour écarter, d'emblée, d'autres questions qui pourraient être soulevées in abstracto relativement à la nature juridique des adresses IP, dans le contexte de la protection de données à caractère personnel.

47. En premier lieu, le Bundesgerichtshof (Cour fédérale de justice) se réfère exclusivement aux « adresses IP dynamiques », à savoir celles qui sont provisoirement attribuées à chaque connexion au réseau et modifiées lors de connexions ultérieures. Sont donc écartées les « adresses IP fixes ou statiques », caractérisées par le fait qu'elles sont invariables et permettent l'identification permanente du dispositif connecté au réseau.

48. En second lieu, la juridiction de renvoi part de la présomption que le fournisseur du site Internet n'est pas, en l'espèce, en mesure d'identifier, au moyen de l'adresse IP dynamique, les personnes qui consultent ses sites et ne dispose pas lui-même d'informations supplémentaires qui, combinées à cette adresse IP, faciliteraient l'identification de ces personnes. Le Bundesgerichtshof (Cour fédérale de justice) semble considérer que, dans ces conditions, l'adresse IP dynamique n'est pas une donnée à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46, *pour le fournisseur du site Internet*.

49. Le doute de la juridiction de renvoi porte sur la possibilité que l'adresse IP dynamique soit qualifiée de donnée à caractère personnel pour le fournisseur du site Internet *si un tiers dispose d'informations supplémentaires* qui, combinées à l'adresse IP dynamique, identifient les personnes consultant ses sites. Cela étant dit, et il s'agit là d'une autre précision intéressante, le Bundesgerichtshof (Cour fédérale de justice) se réfère non pas à tout tiers possédant lesdites informations supplémentaires, mais uniquement au fournisseur d'accès au réseau (il exclut donc d'autres éventuels possesseurs de ce type de données).

50. Ne font donc pas, entre autres, l'objet du débat : a) le point de savoir si les adresses IP statiques sont des données à caractère personnel conformément à la directive 95/46[10] ; b) celui visant à savoir si les adresses IP dynamiques sont, toujours et en toutes circonstances, des données à caractère personnel au sens de cette directive et c) celui consistant à savoir si les adresses IP dynamiques doivent nécessairement être qualifiées de données à caractère personnel lorsqu'un tiers, quel qu'il soit, est capable de les utiliser pour identifier les utilisateurs du réseau.

51. Le point à trancher est par conséquent uniquement celui de savoir si une adresse IP dynamique constitue une donnée à caractère personnel pour le fournisseur d'un service Internet lorsque l'entreprise de communications offrant l'accès au réseau (le fournisseur d'accès) détient des informations supplémentaires qui, combinées à cette adresse, permettent d'identifier la personne accédant au site Internet géré par le premier.

10 — Problème tranché par la Cour dans les arrêts du 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771, point 51), ainsi que du 19 avril 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219). Aux points 51 et 52 de ce dernier arrêt, la Cour a conclu que « la communication, aux fins de son identification, du nom et de l'adresse […] d'un utilisateur d'Internet faisant usage de l'adresse IP à partir de laquelle il est présumé que des fichiers contenant des œuvres protégées ont été illicitement échangés […] constitue un traitement de données à caractère personnel au sens de l'article 2, premier alinéa, de la directive 2002/58, lu en combinaison avec l'article 2, sous b), de la directive 95/46 ».

2. Sur le fond

52. La question à l'origine du présent renvoi préjudiciel fait l'objet d'un débat intense dans la doctrine et la jurisprudence allemandes, polarisé en deux courants d'opinion [11]. Selon le premier (qui opte pour un critère « objectif » ou « absolu »), un utilisateur est identifiable (et l'adresse IP constitue dès lors une donnée à caractère personnel susceptible d'être protégée) lorsque, quels que soient les capacités et les moyens du fournisseur du service Internet, l'utilisateur peut être identifié par la seule combinaison de cette adresse IP dynamique avec des informations fournies par un tiers (par exemple, le fournisseur d'accès au réseau).

53. Pour les partisans de l'autre courant (qui prônent un critère « relatif »), la possibilité de conter sur l'aide d'un tiers pour l'identification finale de l'utilisateur ne suffit pas pour doter l'adresse IP dynamique d'un caractère personnel. L'élément pertinent est la capacité de celui ayant accès à l'information de s'en servir, par ses propres moyens, et d'identifier ainsi une personne.

54. Quels que soient les termes de cette controverse en droit allemand, la réponse de la Cour doit se limiter à l'interprétation des deux dispositions de la directive 95/46 qui ont été citées par la juridiction a quo et par les parties à la procédure, à savoir l'article 2, sous a) [12], et le considérant 26 [13] de cette directive.

55. Du simple fait qu'elles donnent des informations sur la date et l'heure d'accès à un site Internet depuis un ordinateur (ou un autre dispositif), les adresses IP dynamiques révèlent certains traits du comportement des utilisateurs d'Internet et peuvent dès lors constituer une ingérence dans le droit au respect de la vie privée [14] garanti par l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et par l'article 7 de la Charte, au regard desquels, ainsi qu'à celui de l'article 8 de la Charte, la directive 95/46 doit être interprétée [15]. En réalité, les parties au litige ne remettent pas en cause cette prémisse, qui ne fait pas non plus l'objet, en tant que telle, de la demande préjudicielle.

56. La personne sur laquelle ces détails portent n'est pas une « personne physique identifiée ». La date et l'heure d'une connexion ainsi que son origine numérique ne révèlent pas directement et immédiatement l'identité de la personne physique propriétaire du dispositif à partir duquel la consultation du site Internet a lieu ni celle de l'utilisateur l'employant (il peut s'agir de n'importe quelle personne physique).

11 — Voir, sur les deux positions doctrinales, notamment, Schreibauer, M., dans *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., et von Lewinski, K. (éd.), Carl Heymanns Verlag/Wolters Kluwer, Cologne, 2014, 4e éd., § 11, Telemediengesetz (4 à 10). Nink, J., et Pohle, J., « Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze », dans *Multimedia und Recht*, 9/2015, p. 563 à 567. Heidrich, J., et Wegener, C., « Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging », dans *Multimedia und Recht*, 8/2015, p. 487 à 492. Leisterer, H., « Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr », dans *Computer und Recht*, 10/2015, p. 665 à 670.

12 — Reproduit au point 13 des présentes conclusions.

13 — Reproduit au point 11 des présentes conclusions.

14 — Cela a été rappelé par l'avocat général Cruz Villalón au point 76 des conclusions qu'il a présentées dans l'affaire Scarlet Extended (C-70/10, EU:C:2011:255), et c'est également la position adoptée par le contrôleur européen de la protection des données dans son avis, du 22 février 2010, sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC) (JO 2010, C 147, p. 1, point 24) et dans son avis, du 10 mai 2010, sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI (JO 2010, C 323, p. 6, point 11).

15 — Voir à cet égard arrêt du 20 mai 2003, Österreichischer Rundfunk e.a. (C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 68), ainsi que points 51 et suiv. des conclusions que l'avocat général Kokott a présentées dans l'affaire Promusicae (C-275/06, EU:C:2007:454).

57. Toutefois, dans la mesure où une adresse IP dynamique aide (soit à elle seule, soit combinées à d'autres informations) à déterminer qui est le propriétaire du dispositif utilisé pour accéder au site Internet, elle peut être qualifiée d'information sur une « personne identifiable» [16].

58. Selon le Bundesgerichtshof (Cour fédérale de justice), l'adresse IP dynamique n'est pas suffisante, à elle seule, pour identifier l'utilisateur qui a accédé, à travers elle, à un site Internet. Si le fournisseur du service Internet pouvait, au contraire, identifier l'utilisateur grâce à l'adresse IP dynamique, cette dernière serait sans nul doute une donnée à caractère personnel au sens de la directive 95/46. Il ne semble toutefois pas que ce soit le sens de la demande préjudicielle, qui sous-entend que les fournisseurs de services Internet en cause dans le litige au principal ne peuvent pas identifier l'utilisateur exclusivement au moyen de l'adresse IP dynamique.

59. Combinée à d'autres informations, l'adresse IP dynamique facilite l'identification « indirecte » de l'utilisateur, comme toutes les parties le conviennent. L'éventualité de l'existence de ces informations supplémentaires pouvant être combinées à l'adresse IP dynamique autorise-t-elle, purement et simplement, à considérer cette dernière comme constituant une donnée à caractère personnel au sens de la directive ? Il conviendra de déterminer si, à cette fin, la simple possibilité abstraite de connaître ces informations suffit ou si, au contraire, il est nécessaire qu'elles soient à la disposition de celui qui connaît déjà l'adresse IP dynamique ou d'un tiers.

60. Les parties ont centré leurs observations sur l'interprétation du considérant 26 de la directive 95/46, où figure l'expression « moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ». La question de la juridiction de renvoi ne porte pas sur des informations supplémentaires détenues par les fournisseurs de services en cause dans la procédure au principal. Elle ne mentionne pas non plus un quelconque tiers possédant ces informations supplémentaires (dont la combinaison avec l'adresse IP dynamique facilite l'identification de l'utilisateur), mais se réfère au fournisseur d'accès au réseau.

61. Il n'est donc pas nécessaire, en l'espèce, que la Cour analyse tous les moyens qui pourraient « raisonnablement » être mis en œuvre par la partie défenderesse dans la procédure au principal pour que les adresses IP dynamiques dont elle dispose puissent être qualifiées de données à caractère personnel. Puisque le Bundesgerichtshof (Cour fédérale de justice) se réfère uniquement à des informations supplémentaires détenues par un tiers, on peut en déduire a) soit que la défenderesse ne détient pas d'informations supplémentaires susceptibles de permettre l'identification de l'utilisateur, b) soit que, si elle détient de telles informations, elle n'est pas en mesure de les mettre raisonnablement en œuvre à cette fin, en tant que responsable de leur traitement, conformément au considérant 26 de la directive.

62. Les deux hypothèses dépendent d'une constatation factuelle qui ne peut être faite que par la juridiction de renvoi. La Cour pourrait fournir à cette dernière des critères généraux d'interprétation de l'expression « moyens susceptibles d'être raisonnablement mis en œuvre […] par le responsable du traitement », si le Bundesgerichtshof (Cour fédérale de justice) avait des doutes quant à la capacité de la défenderesse à se servir raisonnablement d'informations supplémentaires lui étant propres. Puisque tel n'est pas le cas, il est selon moi hors de propos que la Cour fixe des critères d'interprétation qui ne sont pas nécessaires pour la juridiction de renvoi et que cette dernière n'a pas demandés.

16 — On peut présumer que, sauf preuve du contraire, cette personne est celle qui a navigué sur Internet et accédé au site Internet correspondant. Même abstraction faite de cette dernière présomption, les informations relatives à la date, l'heure et l'origine numérique de l'accès à un site Internet permettraient de mettre ledit accès en lien avec le propriétaire du dispositif et de l'associer indirectement au comportement sur le réseau. L'exception envisageable serait les adresses IP attribuées à des ordinateurs se trouvant dans des endroits tels que les cybercafés, dont les utilisateurs anonymes ne sont pas identifiables et dont le trafic ne donne aucune information personnelle pertinente sur les propriétaires. C'est en outre la seule exception au principe selon lequel les adresses IP sont des données à caractère personnel admise par le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, créé par la directive 95/46 (dit « groupe de travail "article 29" »). L'avis 4/2007 de ce groupe, du 20 juin 2007, sur la notion de « données à caractère personnel » peut être consulté à l'adresse suivante :
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

63. Le cœur de la question posée se limite donc à déterminer si le fait qu'un tiers bien spécifique (le fournisseur d'accès à Internet) dispose d'informations supplémentaires qui, combinées aux adresses IP dynamiques, sont susceptibles de permettre l'identification de l'utilisateur qui a consulté un site Internet déterminé est pertinent aux fins de qualifier lesdites adresses de données à caractère personnel.

64. Il convient à nouveau de mentionner le considérant 26 de la directive 95/46. L'expression « moyens susceptibles d'être raisonnablement mis en œuvre […] *par une autre personne*» [17] pourrait conforter une interprétation selon laquelle il suffirait qu'un tiers puisse obtenir des informations supplémentaires (susceptibles d'être combinées avec une adresse IP dynamique aux fins d'identifier une personne) pour considérer que cette adresse constitue eo ipso une donnée à caractère personnel.

65. Cette interprétation maximaliste conduirait en pratique à considérer tout type d'informations, même insuffisantes en soi pour faciliter l'identification d'un utilisateur, comme constituant des données à caractère personnel. On ne pourra jamais écarter, avec une certitude absolue, la possibilité qu'existe un tiers possédant des informations supplémentaires susceptibles d'être combinées aux premières et d'être dès lors aptes à révéler l'identité d'une personne.

66. Selon moi, la possibilité que les progrès techniques ouvrent sensiblement, dans un futur plus ou moins proche, la voie à l'accès à des instruments toujours plus sophistiqués permettant d'obtenir et de traiter les informations justifie les précautions prises en vue d'anticiper la protection de la vie privée. Lors de la définition des catégories juridiques pertinentes dans le domaine de la protection des données, on a tenté d'inclure des hypothèses de comportement suffisamment larges et flexibles pour couvrir n'importe quel cas envisageable [18].

67. Je crois toutefois que cette préoccupation (qui est par ailleurs tout à fait légitime) ne peut conduire à ignorer les termes de la volonté réglementaire du législateur et que l'interprétation systématique du considérant 26 de la directive 95/46 se limite aux « moyens susceptibles d'être raisonnablement mis en œuvre » *par certains tiers*.

68. Tout comme le considérant 26 mentionne non pas tous les moyens pouvant être mis en œuvre par le responsable du traitement (en l'occurrence, le fournisseur de services Internet), mais uniquement ceux susceptibles d'être « raisonnablement » mis en œuvre, il convient de même de considérer que le législateur se réfère aux « tiers » auxquels le responsable du traitement souhaitant obtenir les informations supplémentaires en vue de l'identification peut, *également de manière raisonnable*, s'adresser. Ce ne serait pas le cas si le contact avec ces tiers était, de fait, très coûteux en termes humains et financiers, pratiquement irréalisable ou interdit par la loi. Sinon, comme je l'indiquais précédemment, il serait presque impossible de faire la distinction entre certains moyens et d'autres, car il serait toujours possible d'imaginer l'existence de cas dans lesquels un tiers, même inaccessible au fournisseur de services Internet, puisse disposer (actuellement ou dans le futur) d'informations supplémentaires pertinentes aux fins d'aider à identifier un utilisateur.

69. Comme indiqué précédemment, le tiers auquel se réfère le Bundesgerichtshof (Cour fédérale de justice) est un fournisseur d'accès au réseau. C'est assurément au tiers auquel il est plus raisonnable de penser que le prestataire de services s'adressera pour collecter les informations supplémentaires nécessaires s'il souhaite identifier de la manière la plus efficace, pratique et directe possible l'utilisateur qui a accédé à son site Internet grâce à l'adresse IP dynamique. Ce n'est en aucun cas un tiers hypothétique, inconnu et inaccessible, mais il s'agit d'un protagoniste principal sur la toile

17 — Mise en italique par mes soins.

18 — Cette vocation de protection et de prévention constitue le fondement de la position défendue par le groupe de travail « article 29 », pour lequel il y a lieu, comme je l'ai indiqué, de partir du principe que les adresses IP constituent une donnée à caractère personnel, la seule exception admise étant l'hypothèse dans laquelle le fournisseur de services est en mesure de déterminer avec une certitude absolue qu'il s'agit d'adresses correspondant à des personnes non identifiables, comme les utilisateurs d'un cybercafé. Voir note en bas de page 16, in fine.

Internet, dont on sait avec certitude qu'il détient les informations nécessaires au fournisseur de services pour identifier un utilisateur. De fait, comme l'indique la juridiction de renvoi, c'est à ce tiers concret que la défenderesse au principal souhaite s'adresser pour collecter les informations supplémentaires qui lui sont indispensables.

70. Le tiers visé au considérant 26 de la directive 95/46 est typiquement le fournisseur d'accès à Internet, auquel le fournisseur de services de la procédure au principal peut le plus « raisonnablement » s'adresser. Il convient toutefois de déterminer si l'obtention des informations supplémentaires détenues par ce tiers peut être qualifiée de « raisonnablement » viable ou réalisable.

71. Le gouvernement allemand affirme que, puisque les informations détenues par le fournisseur d'accès à Internet constituent des données à caractère personnel, ce dernier ne peut les fournir purement et simplement. Il ne peut le faire que conformément à la réglementation régissant le traitement de ces données [19].

72. Il en va sans aucun doute ainsi, car, pour pouvoir jouir de ces informations, il convient de se conformer à la législation applicable en matière de données à caractère personnel. Une information ne peut être « raisonnablement » obtenue que dans le respect des conditions régissant l'accès à ce type d'informations, la première d'entre elles étant la possibilité légale de leur conservation et de leur transmission à d'autres personnes. Le fournisseur d'accès à Internet a certes la possibilité de refuser de remettre les informations concernées, mais le contraire est aussi possible. Du seul fait de la possibilité de transmission d'informations, parfaitement « raisonnable », l'adresse IP dynamique devient, conformément aux termes du considérant 26 de la directive 95/46, une donnée à caractère personnel pour le fournisseur de services Internet.

73. Il s'agit d'une éventualité pouvant être réalisée *dans le cadre de la loi* et donc « raisonnable ». Les moyens d'accès raisonnables visés dans la directive 95/46 doivent, par définition, être des moyens licites [20]. C'est, bien entendu, la prémisse sur laquelle la juridiction de renvoi se fonde, comme le rappelle le gouvernement allemand [21]. Cela réduit significativement les voies d'accès juridiquement pertinentes, car elles doivent nécessairement être licites. Néanmoins tant que ces dernières existent, même si leur application pratique s'avère restrictive, elles constituent un « moyen raisonnable » au sens de la directive 95/46.

74. Par conséquent, je considère que, dans les termes posés par le Bundesgerichtshof (Cour fédérale de justice), il convient de répondre à sa première question par l'affirmative. L'adresse IP dynamique doit être considérée comme étant une donnée à caractère personnel pour le fournisseur de services Internet, compte tenu de l'existence d'un tiers (le fournisseur d'accès au réseau) auquel le premier peut raisonnablement s'adresser pour obtenir des informations supplémentaires qui, combinées à l'adresse IP dynamique, permettraient d'identifier un utilisateur.

75. J'estime que le résultat qu'aurait la solution contraire à celle que je propose renforce cette dernière. Si les adresses IP dynamiques ne constituaient pas des données à caractère personnel pour le fournisseur de services Internet, celui-ci pourrait les conserver sans limite de temps et pourrait à tout moment demander au fournisseur d'accès Internet les informations supplémentaires afin de les combiner à l'adresse IP dynamique et d'identifier l'utilisateur. Dans ces circonstances, comme le

19 — Points 40 et 45 de ses observations écrites.

20 — À cet égard, le fait que l'accès aux données à caractère personnel soit possible de facto, en violation des lois en matière de protection des données, est dénué de pertinence.

21 — Points 47 et 48 de ses observations écrites.

reconnaît le gouvernement allemand [22], l'adresse IP dynamique deviendrait une donnée à caractère personnel, dans la mesure où le fournisseur de services Internet détiendrait les informations supplémentaires permettant d'identifier l'utilisateur. Dans un tel cas, la législation en matière de protection des données s'appliquerait.

76. Cela étant dit, il s'agirait d'une donnée dont la conservation n'aurait été possible que dans la mesure où elle n'aurait jusqu'alors pas été considérée comme constituant une donnée à caractère personnel pour le fournisseur de services. La qualification juridique de l'adresse IP dynamique en tant que donnée à caractère personnel dépendrait donc du bon vouloir de ce dernier et serait subordonnée à l'éventualité que, dans le futur, il décide d'utiliser l'adresse IP dynamique pour identifier l'utilisateur en la combinant avec les informations supplémentaires collectées auprès d'un tiers. Selon moi, l'élément déterminant, conformément à la directive 95/46, est toutefois la possibilité (raisonnable) de l'existence d'un tiers « accessible » possédant les moyens nécessaires pour permettre l'identification d'une personne, et non pas la matérialisation de la possibilité de recourir à ce tiers.

77. On pourrait même admettre, à l'instar du gouvernement allemand, que l'adresse IP dynamique ne devient une donnée à caractère personnel que lorsque le fournisseur d'accès à Internet la reçoit. Il faudrait toutefois alors reconnaître le caractère rétroactif de cette qualification, par rapport au délai de conservation de l'adresse IP, et, dès lors, considérer l'absence d'une telle qualification si le délai durant lequel la donnée aurait pu être conservée si elle avait d'emblée été qualifiée de donnée à caractère personnel a expiré. Dans ce cas de figure, on obtiendrait un résultat contraire à l'esprit de la législation en matière de protection des données à caractère personnel. Ne pas reconnaître d'emblée la pertinence d'une caractéristique que ces données présentent depuis le début méconnaîtrait la raison justifiant leur conservation uniquement provisoire : leur aptitude à identifier (en soi ou en combinaison avec d'autres données) une personne physique. Pour cette raison aussi, purement économique, il est plus raisonnable de leur attribuer ce caractère d'emblée.

78. Par conséquent, à titre de première conclusion, je considère que l'article 2, sous a), de la directive 95/46 doit être interprété en ce sens qu'une adresse IP enregistrée par un fournisseur de services à l'occasion d'un accès à son site Internet constitue pour celui-ci une donnée à caractère personnel, dans la mesure où un fournisseur d'accès au réseau (Internet) dispose des informations supplémentaires nécessaires pour identifier la personne concernée.

### B – *Sur la seconde question*

79. Par la seconde question préjudicielle, le Bundesgerichtshof (Cour fédérale de justice) souhaite savoir si l'article 7, sous f), de la directive 95/46 s'oppose à une réglementation nationale qui ne permet la collecte et l'utilisation des données à caractère personnel afférentes à un utilisateur, sans le consentement de celui-ci, que dans la mesure où cela est nécessaire pour permettre et facturer l'utilisation concrète du média électronique par l'utilisateur en question, la finalité consistant à garantir la capacité générale de fonctionnement du média électronique ne pouvant pas justifier l'utilisation des données après la fin de chaque session.

80. Avant de répondre, il convient d'apporter une précision sur l'information donnée par le Bundesgerichtshof (Cour fédérale de justice), selon laquelle les données litigieuses sont conservées afin de garantir le bon fonctionnement des sites Internet en cause dans la procédure au principal, rendant le cas échéant possibles les poursuites pénales contre les attaques cybernétiques dont ces sites pourraient faire l'objet.

22 — Point 36 de ses observations écrites.

81. Il convient donc avant tout de se demander si le traitement des adresses IP visées par le renvoi relève de l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 [23].

1. Sur l'applicabilité de la directive 95/46 au traitement des données litigieuses

82. Il semble que la République fédérale d'Allemagne intervienne dans la procédure au principal en tant que simple fournisseur de services Internet, c'est-à-dire en tant que particulier (et donc sine imperio). Il en découle que, en principe, le traitement des données faisant l'objet du présent litige n'est pas exclu du champ d'application de la directive 95/46.

83. Aux termes de la Cour dans l'arrêt Lindqvist [24], les activités visées à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 « sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers» [25]. Dans la mesure où le responsable du traitement des données en cause agit en fait, malgré sa condition d'autorité publique, comme un sujet privé, la directive 95/46 est applicable.

84. Lorsqu'elle souligne la finalité principale que l'administration allemande vise en enregistrant les adresses IP dynamiques, la juridiction de renvoi indique que ladite administration entend « garantir et maintenir la sécurité et le bon fonctionnement de ses médias électroniques », notamment « la reconnaissance et la lutte contre les fréquentes attaques par "déni de service" dans le cadre desquelles l'infrastructure des médias électroniques est paralysée par l'inondation (flood) ciblée et coordonnée de certains serveurs Internet par un grand nombre de demandes» [26]. La conservation des adresses IP dynamiques à cette fin est commune à tout propriétaire de sites Internet d'une certaine importance et n'implique ni directement ni indirectement l'exercice du pouvoir public ; par conséquent, inclure une conservation à cette fin dans le champ d'application de la directive 95/46 ne présente pas de difficulté majeure.

85. Le Bundesgerichtshof (Cour fédérale de justice) affirme toutefois que la conservation des adresses IP dynamiques par les fournisseurs de services en cause dans la procédure au principal vise également à poursuivre pénalement, le cas échéant, les auteurs d'éventuelles attaques cybernétiques. Cette finalité suffit-elle pour exclure le traitement de ces données du champ d'application de la directive 95/46 ?

86. Selon moi, si l'on entendait par « poursuites pénales » l'exercice du ius puniendi de l'État par les fournisseurs de services défendeurs dans la procédure au principal, il s'agirait d'une « activité de l'État relative à des domaines du droit pénal », et donc de l'une des exceptions prévues à l'article 3, paragraphe 2, premier tiret, de la directive 95/46.

87. Dans ces circonstances, conformément à la jurisprudence établie par la Cour dans l'affaire Huber [27], le traitement de données à caractère personnel par les fournisseurs de services aux fins de la sécurité et du fonctionnement technique de leurs médias électroniques relèverait du champ d'application de la directive 95/46, alors que le traitement des données visant à l'activité de l'État en matière pénale en serait exclu.

23 — N'entrent pas dans le champ d'application de la directive 95/46 les « traitements [de données à caractère personnel] ayant pour objet la sécurité publique, la défense, la sûreté de l'État […] et *les activités de l'État relatives à des domaines du droit pénal* » (mise en italique par mes soins).

24 — Arrêt du 6 novembre 2003 (C-101/01, EU:C:2003:596, point 43).

25 — Voir, dans les mêmes termes, arrêt du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia (C-73/07, EU:C:2008:727, point 41).

26 — Point 36 de la décision de renvoi préjudiciel.

27 — Arrêt du 16 décembre 2008 (C-524/06, EU:C:2008:724, point 45).

88. En outre, même si les poursuites pénales proprement dites n'incombaient pas à la République fédérale d'Allemagne, en tant que simple fournisseur de services n'agissant pas dans l'exercice du pouvoir public, et que celle-ci se contentait, comme n'importe quel particulier, de transférer les adresses IP litigieuses à un organe étatique en vue de l'exercice d'une action répressive, le traitement des adresses IP dynamiques aurait également pour objet une activité exclue du champ d'application de la directive 95/46.

89. C'est ce qui ressort de la jurisprudence établie dans l'affaire Parlement/Conseil et Commission [28], dans laquelle la Cour a affirmé que le fait que certaines données à caractère personnel « ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un États tiers » ne signifie pas que ce transfert « n'entre pas dans le champ d'application » de l'article 3, paragraphe 2, premier tiret, de la directive 95/46, lorsque la finalité du transfert a pour objet l'activité de l'État relative à des domaines du droit pénal, dans la mesure où, dans cette affaire, le transfert « s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique» [29].

90. Au contraire, si, comme je le pense, il convient d'entendre par « poursuites pénales », comme il ressort de la décision de renvoi, l'action propre à un particulier en tant que personne habilitée à demander, au moyen de l'action correspondante, l'application du ius puniendi par l'État, il ne saurait être affirmé que le traitement des adresses IP dynamiques a pour objet l'activité de l'État relative à des domaines du droit pénal, exclue du champ d'application de la directive 95/46.

91. En effet, la conservation et l'enregistrement de telles données constitueraient un moyen supplémentaire de preuve à l'appui de la demande, faite à l'État par le propriétaire du site Internet, de sanctionner un comportement illicite. Il s'agirait, en définitive, d'un instrument de protection, par la voie pénale, des droits reconnus par l'ordre juridique à un particulier (en l'occurrence, une entité publique agissant selon un régime de droit privé). Sous cet angle, il n'y a là aucune différence avec l'initiative de n'importe quel autre fournisseur de services Internet demandant la protection de l'État conformément aux procédures d'exercice de l'action pénale prévues par l'ordre juridique.

92. Par conséquent, si l'administration allemande se comporte comme un fournisseur de services Internet dépourvu de pouvoir public, point qu'il appartient à la juridiction de renvoi de trancher, le traitement qu'elle fait des adresses IP dynamiques, en tant que données à caractère personnel, relève du champ d'application de la directive 95/46.

2. Sur le fond

93. L'article 15, paragraphe 1, de la TMG n'autorise la collecte et l'utilisation des données à caractère personnel d'un utilisateur que dans la mesure où cela est nécessaire pour permettre et facturer une utilisation concrète du média électronique. Plus précisément, le fournisseur de services ne peut collecter et utiliser que les données dites d'utilisation, à savoir les données à caractère personnel d'un utilisateur indispensables pour « permettre et facturer l'utilisation des médias électroniques ». Ces données doivent être supprimées dès la fin de l'opération (donc dès que cesse l'utilisation concrète du média électronique), à moins qu'elles ne doivent être conservées « à des fins de facturation », conformément à l'article 15, paragraphe 4, de la TMG.

28 — Arrêt du 30 mai 2006 (C-317/04 et C-318/04, EU:C:2006:346, points 54 à 59).

29 — Arrêt du 30 mai 2006 (C-317/04 et C-318/04, EU:C:2006:346, point 59).

94. Une fois qu'il a été mis fin à la connexion, l'article 15 de la TMG semble s'opposer à l'enregistrement des données d'utilisation pour d'autres raisons, y compris pour garantir « l'utilisation des médias électroniques » de manière générale. Puisque cette disposition se réfère exclusivement à la facturation comme cause justifiant la conservation des données, elle pourrait être comprise (bien que son interprétation définitive incombe à la juridiction de renvoi) comme exigeant que les données d'utilisation ne soient employées que pour permettre une utilisation concrète, et supprimées lorsque cette dernière s'achève.

95. L'article 7, sous f), de la directive 95/46 [30] justifie le traitement de données à caractère personnel dans des termes que je qualifierais de plus généreux (pour le responsable du traitement) que ceux prévus dans le libellé de l'article 15 de la TMG. La disposition allemande peut être taxée, sur ce point, de disposition plus restrictive que celle de l'Union, car elle ne prévoit pas, en principe, la réalisation d'un autre intérêt légitime que celui lié à la facturation du service, alors que, en tant que fournisseur de services Internet, la République fédérale d'Allemagne pourrait également avoir un intérêt légitime à garantir le bon fonctionnement de ses sites Internet au-delà de chaque utilisation concrète [31].

96. La jurisprudence de la Cour dans l'arrêt ASNEF et FECEMD [32] fournit les éléments pour répondre à la seconde question préjudicielle. La Cour y a affirmé qu'il découle de l'objectif visé par la directive 95/46 « que l'article 7 de la directive 95/46 prévoit une liste exhaustive et limitative des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite» [33]. Il s'ensuit que « les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la directive 95/46 ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article» [34].

97. L'article 15 de la TMG n'ajoute pas d'exigence supplémentaire à celles prévues à l'article 7 de la directive 95/46 pour la licéité du traitement de données (contrairement à ce qui s'est passé dans les affaires ASNEF et FECEMD [35]), mais, s'il est interprété dans le sens restrictif indiqué par la juridiction de renvoi, il limite le contenu de la condition prévue à l'article 7, sous f) : alors que le législateur de l'Union se réfère, de manière générale, à la « réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées », l'article 15 de la TMG satisfait uniquement la nécessité visant à « permettre et facturer l'utilisation [concrète] des médias électroniques ».

98. Tout comme dans les affaires ASNEF et FECEMD [36], en l'espèce aussi, une mesure nationale (répétons-le, si elle était interprétée dans le sens restrictif expliqué ci-dessus) modifierait la portée d'un principe de l'article 7 de la directive 95/46 au lieu de se contenter de la préciser, seul point sur lequel les autorités de chaque État membre disposent d'un certain pouvoir d'appréciation, conformément à l'article 5 de la directive 95/46.

30 — Reproduit au point 17 des présentes conclusions.

31 — Voir point 84 des présentes conclusions. Les propriétaires des sites Internet ont assurément un intérêt légitime à prévenir et combattre les « dénis de service » mentionnés par la juridiction de renvoi, à savoir les attaques massives qui sont parfois lancées de manière concertée contre certains sites Internet afin de les saturer et de les rendre inopérants.

32 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777).

33 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777, point 30).

34 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777, point 32).

35 — Dans cette affaire, la législation nationale ajoutait aux exigences de l'article 7, sous f), de la directive 95/46 celle imposant que les données faisant l'objet du traitement figurent dans des sources accessibles au public.

36 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777).

99. En effet, aux termes de cette dernière disposition, «[l]es États membres précisent, dans les limites des dispositions du présent chapitre [37], les conditions dans lesquelles les traitements de données à caractère personnel sont licites». Toutefois, comme la Cour l'a affirmé dans les affaires ASNEF et FECEMD [38], « au titre de l'article 5 de la directive 95/46, les États membres ne sauraient non plus introduire d'autres principes relatifs à la légitimation des traitements de données à caractère personnel que ceux énoncés à l'article 7 de cette directive ni modifier, par des exigences supplémentaires, la portée des six principes prévus audit article 7 ».

100. L'article 15 de la TMG réduirait substantiellement, par rapport à l'article 7, sous f), de la directive 95/46, la portée de l'intérêt légitime pertinent pour justifier le traitement de données, sans se contenter de la préciser ou de la nuancer dans le cadre de ce qui est autorisé à l'article 5 de la directive 95/46. Il le ferait, en outre, de manière catégorique et absolue, sans permettre que la protection et la garantie de l'utilisation générale du média électronique puissent faire l'objet d'une pondération avec « l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 » de la directive 95/46, conformément à l'article 7, sous f), de celle-ci.

101. En définitive, tout comme dans les affaires ASNEF et FECEMD [39], le législateur allemand aurait prescrit, pour certaines catégories de données à caractère personnel, « de manière définitive le résultat de la pondération des droits et intérêts opposés, sans permettre un résultat différent en raison de circonstances particulières d'un cas concret », de sorte qu'« il ne s'agit plus d'une précision au sens [de l']article 5 » de la directive 95/46.

102. Dans ces conditions, je considère que le Bundesgerichtshof (Cour fédérale de justice) est tenu d'interpréter la législation nationale conformément à la directive 95/46, ce qui implique a) la possibilité d'inclure, parmi les raisons justifiant le traitement des données dites « d'utilisation », l'intérêt légitime du fournisseur de médias électroniques de protéger l'utilisation générale de ceux-ci et b) la possibilité de procéder, au cas par cas, à une pondération de cet intérêt du fournisseur du service avec l'intérêt ou les droits et libertés fondamentaux de l'utilisateur, afin de déterminer lequel mérite protection conformément à l'article 1er, paragraphe 1, de la directive 95/46 [40].

103. Il n'y a selon moi plus rien à ajouter sur la manière selon laquelle cette pondération doit avoir lieu dans l'affaire à l'origine du présent renvoi préjudiciel. Le Bundesgerichtshof (Cour fédérale de justice), préoccupé par la réponse à une question préalable, à savoir si une telle pondération peut avoir lieu, ne pose aucune question à ce sujet.

104. Enfin, il semble superflu d'indiquer que le juge a quo peut tenir compte des éventuelles mesures législatives adoptées par l'État membre dans le cadre de l'autorisation prévue à l'article 13, paragraphe 1, sous d), de la directive 95/46 pour limiter la portée des obligations et des droits prévus à l'article 6, lorsque cela est nécessaire pour sauvegarder, entre autres, « […] la prévention, la recherche, la détection et la poursuite d'infractions pénales […] ». La juridiction de renvoi ne se réfère pas non plus à ce point, consciente sans nul doute de l'existence des deux articles.

37 — Chapitre II, intitulé « Conditions générales de licéité des traitements de données à caractère personnel », qui contient les articles 5 à 21 de la directive 95/46.

38 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777, point 36).

39 — Arrêt du 24 novembre 2011 (C-468/10 et C-469/10, EU:C:2011:777, point 47).

40 — Lors de l'audience, les avocats de M. Breyer ont contesté la nécessité de l'enregistrement des adresses IP dynamiques pour protéger le bon fonctionnement des services Internet face à d'éventuelles attaques. Je ne crois pas qu'il soit possible de répondre en termes absolus à ce problème ; au contraire, il faudrait pour cela procéder préalablement, au cas par cas, à la pondération entre l'intérêt du propriétaire du site Internet et les droits et intérêts des utilisateurs.

105. Par conséquent, je suggère de répondre à la seconde question préjudicielle en ce sens que l'article 7, sous f), de la directive 95/46 s'oppose à une disposition nationale dont l'interprétation ne permet pas à un fournisseur de services de collecter et de traiter les données à caractère personnel afférentes à un utilisateur, sans le consentement de celui-ci, afin de garantir le fonctionnement du média électronique, après la fin de chaque session.

## VI – Conclusion

106. Eu égard aux considérations qui précèdent, je propose à la Cour de répondre aux questions posées comme suit :

1) Conformément à l'article 2, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, une adresse IP (protocole Internet) dynamique par laquelle un utilisateur a accédé au site Internet d'un fournisseur de médias électroniques constitue pour celui-ci une donnée à caractère personnel, dans la mesure où un fournisseur d'accès au réseau possède des informations supplémentaires qui, combinées à l'adresse IP dynamique, permettraient d'identifier l'utilisateur.

2) L'article 7, sous f), de la directive 95/46 doit être interprété en ce sens que l'objectif visant à garantir le fonctionnement du média électronique peut, en principe, être considéré comme un intérêt légitime, dont la réalisation justifie le traitement de cette donnée à caractère personnel, pour autant qu'il prévale sur l'intérêt ou les droits fondamentaux de la personne concernée. Une disposition nationale qui ne permettrait pas de prendre en compte cet intérêt légitime ne serait pas conforme à la disposition précitée.